Amendments to the Claims:

1. (Currently Amended) A method comprising:

providing a plurality of security policies to be applied to traffic at least one of to or from a host, wherein each security policy includes an application instance identifier ~~associated with~~ identifying a security service, at least two application instance identifiers ~~being associated with~~ identifying different, independent security services that ~~operate~~ provide security to packets of data according to different protocols at different layers of a multi-layered protocol stack; and

creating a plurality of security associations in accordance with the security services identified by the application instance identifiers, at least two security associations being created ~~based upon~~ in accordance with respective, ones of the different security services to thereby create a centralized key store including the plurality of security policies and security associations, at least one of the security associations being created according to a key management protocol that differs from the protocols according to which the security services ~~operate~~ provide security.

2. (Currently Amended) A method according to Claim 1 further comprising:

receiving at least one packet of data; and

applying the security service ~~associated with~~ identified by an identified application instance identifier to the at least one packet of data to thereby transform the at least one packet of data, wherein the security service is applied to the at least one packet based upon at least one security policy and at least one security association.

3. (Currently Amended) A method according to Claim 2 further comprising:

receiving the at least one transformed packet of data; and

applying the security service ~~associated with~~ identified by the identified application instance identifier to the at least one transformed packet of data to thereby generate a representation of the at least one packet of data, wherein the security service is applied to the transformed at least one packet based upon at least one security association.

4. (Previously Presented) A method according to Claim 2, wherein providing a plurality of security policies comprises providing at least one security policy further including at least one selector field having at least one selector value in a format common to a plurality of security service protocols, and wherein applying the security service comprises applying the security service further based upon the at least one security policy including the at least one selector value.

5. (Original) A method according to Claim 1, wherein creating at least one security association comprises creating at least one security association according to an Internet Key Exchange (IKE) technique.

6. (Currently Amended) An apparatus comprising:

a processor configured to provide a plurality of security policies to be applied to traffic at least one of to or from the apparatus, wherein each security policy includes an application instance identifier ~~associated with~~ identifying a security service, at least two application instance identifiers ~~being associated with~~ identifying different, independent security services that ~~operate~~ provide security to packets of data according to different protocols at different layers of a multi-layered protocol stack, wherein the processor is configured to apply the security services ~~associated with~~ identified by respective, identified application instance identifiers to packets of data, including ~~applying~~ being configured to apply different security services to at least two different packets of data, to thereby transform the packets of data, wherein the processor is configured to apply the security services to the packets based upon ~~a~~ the plurality of security policies and a plurality of security associations, and

wherein the processor is configured to relay the transformed packets of data to one or more security gateways configured to apply the security services ~~associated with~~ identified by the respective, identified application instance identifiers to the transformed packets of data to thereby generate representations of the respective packets of data.

7. (Currently Amended) An apparatus according to Claim 6, wherein the processor is also configured to create a plurality of security associations in accordance with the security services identified by the application instance identifiers, at least two security associations being created ~~based upon~~ in accordance with respective, ~~-~~ ones of the different security services to thereby create a centralized key store including the plurality of security policies and security associations, at least one of the security associations being created according to a key management protocol that differs from the protocols according to which the security services ~~operate~~ provide security.

8. (Previously Presented) An apparatus according to Claim 6, wherein the processor is configured to provide at least one security policy further including at least one selector field having at least one selector value in a format common to a plurality of security service protocols, and wherein the processor is configured to apply a security service further based upon the at least one security policy including the at least one selector value.

9. (Previously Presented) An apparatus according to Claim 6, wherein the processor is configured to relay the transformed packets of data to one or more security gateways configured to receive the transformed packets of data from the processor, and thereafter apply the security services to the transformed packets of data based upon the security associations.

10. (Previously Presented) An apparatus according to Claim 6, wherein the processor is configured to create at least one security association according to an Internet Key Exchange (IKE) technique.

11. (Currently Amended) An apparatus comprising:

a security policy database configured to store a plurality of security policies to be applied to traffic at least one of to or from the apparatus, wherein each security policy includes an application instance identifier ~~associated with~~ identifying a security service, at least two application instance identifiers ~~being associated with~~ identifying different, independent security

services that ~~operate~~ provide security to packets of data according to different protocols at different layers of a multi-layered protocol stack;

a security association database configured to store a plurality of security associations; and

a processor configured to create at least two security associations ~~based upon~~ in accordance with respective~~,~~ ones of the different security services to thereby create a centralized key store including the plurality of security policies and the security associations, at least one of the security associations being created according to a key management protocol that differs from the protocols according to which the security services ~~operate~~ provide security.

12. (Currently Amended) An apparatus according to Claim 11, wherein the processor is configured to receive at least one packet of data, and thereafter apply the security service ~~associated with~~ identified by an identified application instance identifier to the at least one packet of data to thereby transform the at least one packet of data, and wherein the processor is configured to apply the security service to the at least one packet based upon at least one security policy and at least one security association.

13. (Previously Presented) An apparatus according to Claim 12, wherein the security policy database is configured to store at least one security policy further including at least one selector field having at least one selector value in a format common to a plurality of security service protocols, and wherein the processor is configured to apply the security service further based upon the at least one security policy including the at least one selector value.

14. (Currently Amended) An apparatus according to Claim 11, wherein the processor is also configured to receive at least one transformed packet of data, and thereafter apply the security service ~~associated with~~ identified by an identified application instance identifier to the at least one transformed packet of data to thereby generate a representation of the at least one packet of data, and wherein the processor is configured to apply the security service to the transformed at least one packet based upon at least one security association.

15. (Previously Presented) An apparatus according to Claim 11, wherein the processor is configured to create at least one security association according to an Internet Key Exchange (IKE) technique.

16. (Currently Amended) A computer program product comprising a computer-readable storage medium having computer-readable program code portions stored therein, the computer-readable program portions comprising:

a first executable portion configured to provide a plurality of security policies to be applied to traffic at least one of to or from a host, wherein each security policy includes an application instance identifier ~~associated with~~ identifying a security service, at least two application instance identifiers ~~being associated with~~ identifying different, independent security services that ~~operate~~ provide security to packets of data according to different protocols at different layers of a multi-layered protocol stack; and

a second executable portion configured to create a plurality of security associations in accordance with the security services identified by the application instance identifiers, at least two security associations being created ~~based upon~~ in accordance with respective~~,~~ ones of the different security services to thereby create a centralized key store including the plurality of security policies and security associations, at least one of the security associations being created according to a key management protocol that differs from the protocols according to which the security services ~~operates~~ provide security.

17. (Currently Amended) A computer program product according to Claim 16 further comprising:

a third executable portion configured to receive at least one packet of data; and

a fourth executable portion configured to apply the security service ~~associated with~~ identified by an identified application instance identifier to the at least one packet of data to thereby transform the at least one packet of data, wherein the security service is applied to the at least one packet based upon the at least one security policy and the at least one security association.

18. (Previously Presented) A computer program product according to Claim 17, wherein the first executable portion is configured to provide at least one security policy further including at least one selector field having at least one selector value in a format common to a plurality of security service protocols, and wherein the fourth executable portion is configured to apply the security service further based upon the at least one security policy including the at least one selector value.

19. (Currently Amended) A computer program product according to Claim 16 further comprising:

a third executable portion configured to receive at least one transformed packet of data; and

a fourth executable portion configured to apply the security service ~~associated with~~ identified by an identified application instance identifier to the at least one transformed packet of data to thereby generate a representation of the at least one packet of data, wherein the security service is applied to the transformed at least one packet based upon the at least one security association.

20. (Previously Presented) A computer program product according to Claim 16, wherein the second executable portion is configured to create at least one security association according to an Internet Key Exchange (IKE) technique.